

Node Identity Architecture: Handling mobility and multiple technologies

**Bengt Ahlgren, SICS
(joint work with a lot of people)**

AN / Daidalos workshop
NEC, Heidelberg
November 19-20, 2007

Background and motivation

- The Internet network problem was once solved with IPv4
- Since then, the problem has gradually been “unsolved”...
 - ▶ *NATs, firewalls and other middleboxes*
 - ▶ *Nodes and whole networks moving*
 - ▶ *Traffic which make deliberate harm*
- IPv6 is not an alternative
 - ▶ *Besides, we have not managed to migrate to it!*
- We think it is time for a new Internet network architecture!

Architecture goals

- **Bridge over heterogeneous domains**
 - ▶ NATs and firewalls should be first order components
- **Require minimal set of common pieces**
 - ▶ e.g., avoid new global managed address space
 - ▶ must anyway handle domains with different address spaces (IPv4 & IPv6, private & public)
- **Need strong migration incentives** (c.f. IPv6)
 - ▶ Integrated mobility (nodes and nets)
 - ▶ Provide multihoming
 - ▶ NAT traversal
 - ▶ Protection from unwanted traffic (DoS protection)
 - ▶ Benefit from partial deployment

Main ideas

- **Use a *node identity layer***
 - ▶ separation of node identity and node location(s)
 - ▶ using cryptographic identifiers
 - ▶ we call these Node ID or NID
 - ▶ (same as in HIP)
- **“Abuse” the identity layer by doing *routing on the node identifiers***
 - ▶ (not part of HIP)
- (Much of the design is then about handling scalability issues in the NID routing overlay)

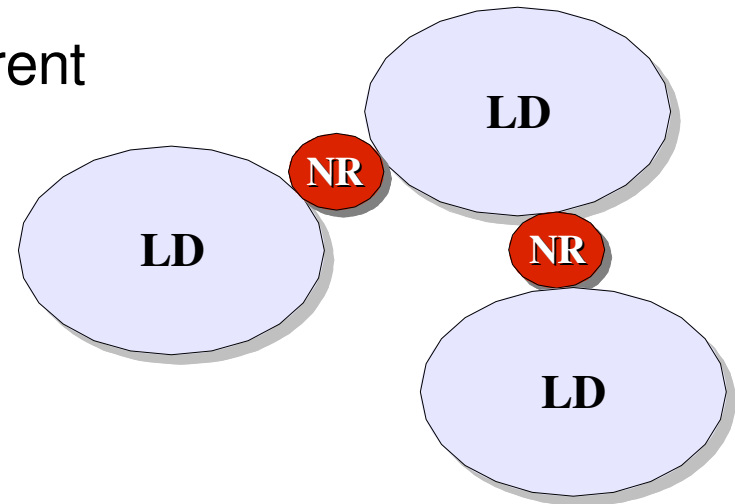
Main concepts

■ Locator domain (LD)

- ▶ world consists of independent LDs
- ▶ LDs are self-contained with coherent internal addressing and routing
- ▶ connectivity between LDs is dynamic

■ Node identity router (NR)

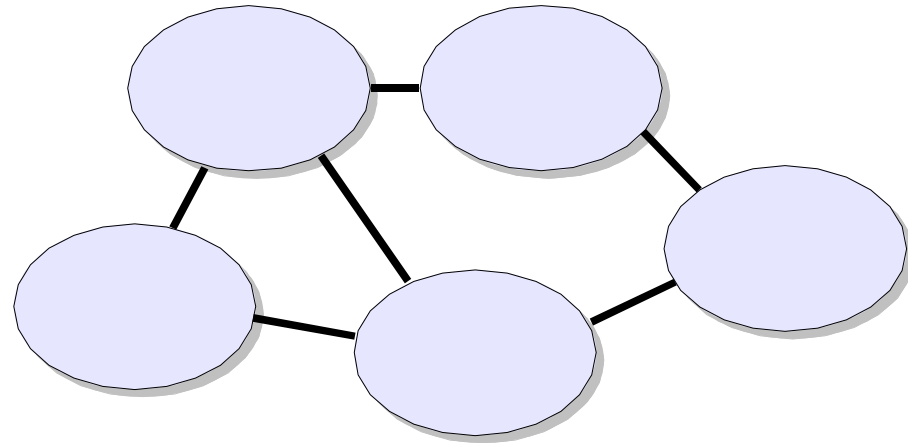
- ▶ aka NID router
- ▶ connects LDs
- ▶ forwards packets using a NID routing table
 - very much like an IP router forward packets using an IP routing table



Handling scalability (1)

- **Unrestricted LD topology creates very, very hard routing problem**

- ▶ BGP-like routing on global dynamic structure and no aggregation...

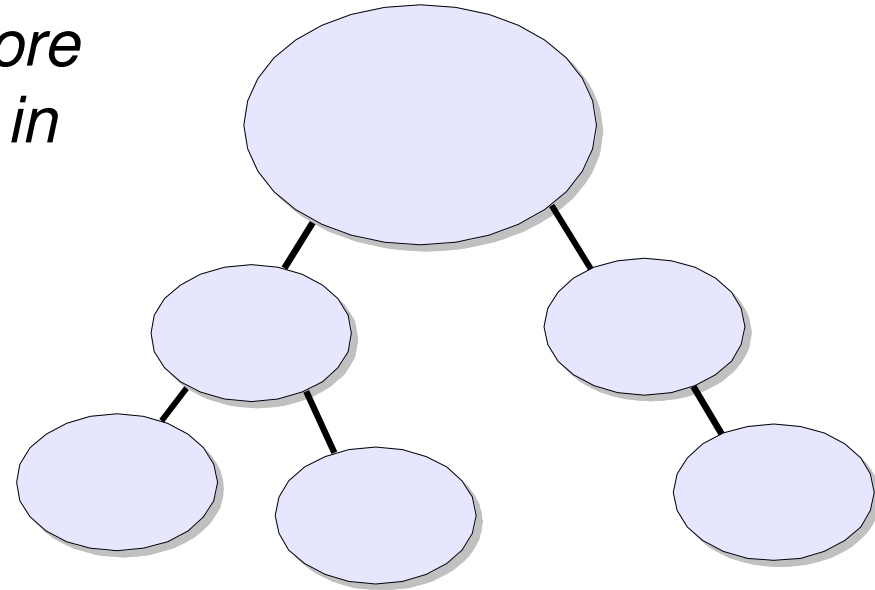


- **Observation:** dynamics is at the network edges

- ▶ host and stub network mobility and multi-homing
- ▶ core networks (LDs) are mostly statically interconnected

Handling scalability (2)

- **Assumption:** *depend on a core LD to which edge LDs attach in tree-like structures*
 - ▶ core LD \approx current Internet (without NAT:ed subnets)
 - ▶ routing in stub trees (DAGs, really) is by default towards the core
 - ▶ nodes have to register up to the core to be reachable
 - ▶ stub trees are of limited size – up to thousands, but not millions, nodes



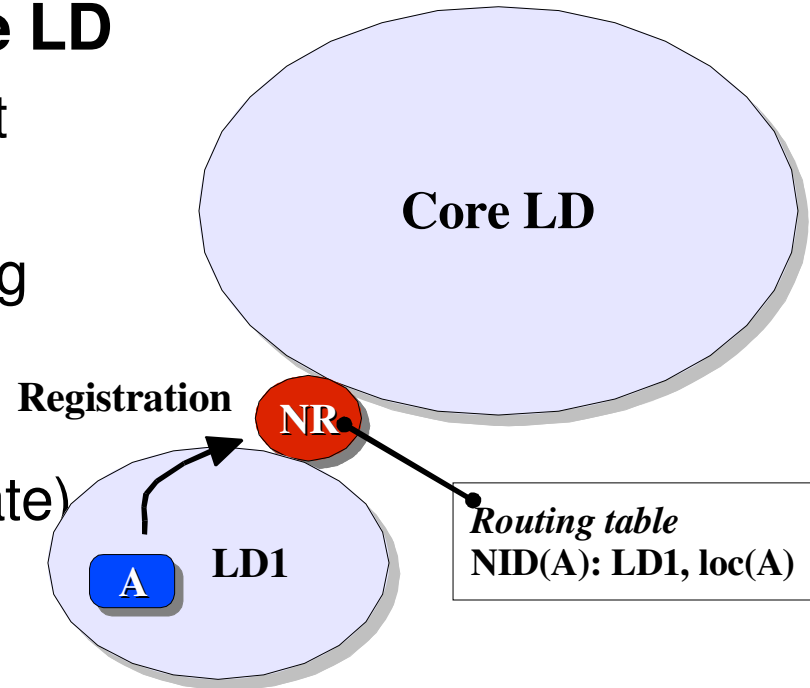
Node registration

■ Nodes register up to the core LD

- ▶ Registration follows the default route to the core
- ▶ Registration establishes routing state in the reverse direction of the default path
- ▶ Registration times out (soft-state) and has to be refreshed

■ Registration is a simple routing protocol

- ▶ More advanced routing schemes can be applied!



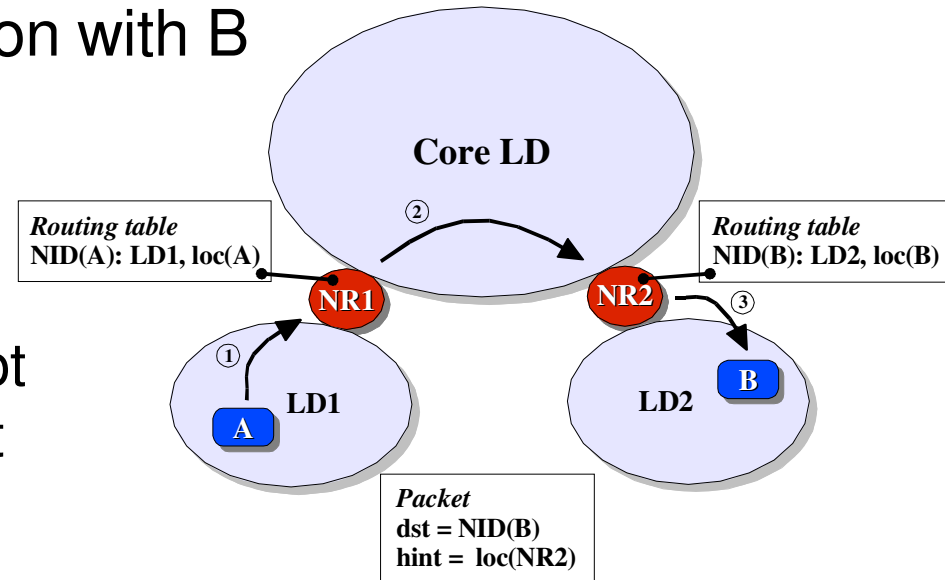
Taking the core hop – routing hints

- Default routes up the trees, registration down the trees
 - ▶ **the “core hop” remains!**
- *Assumption: we do not have a global database with all NID->IP mappings*
- Introduce a **routing hint**:
 - ▶ similar to a partial source route
 - ▶ has to be specified by the source node in packets
 - ▶ when there is no routing info for a destination, try the hint
- Options for the routing hint:
 - ▶ a NID (requires DHT or other db with core NRs NID->IP)
 - ▶ an IP address (no additional machinery needed)

Routing hint example

- A establishes communication with B

- ▶ A specifies $dst = NID(B)$ and routing hint = NR2
- ▶ (1) up tree: default route
- ▶ (2) core hop: NR1 does not have knowledge of B, so it uses the hint
- ▶ (3) down tree: NR2 uses the routing entry it has for B



- (The router the hint points to serves as a home agent or rendezvous server)

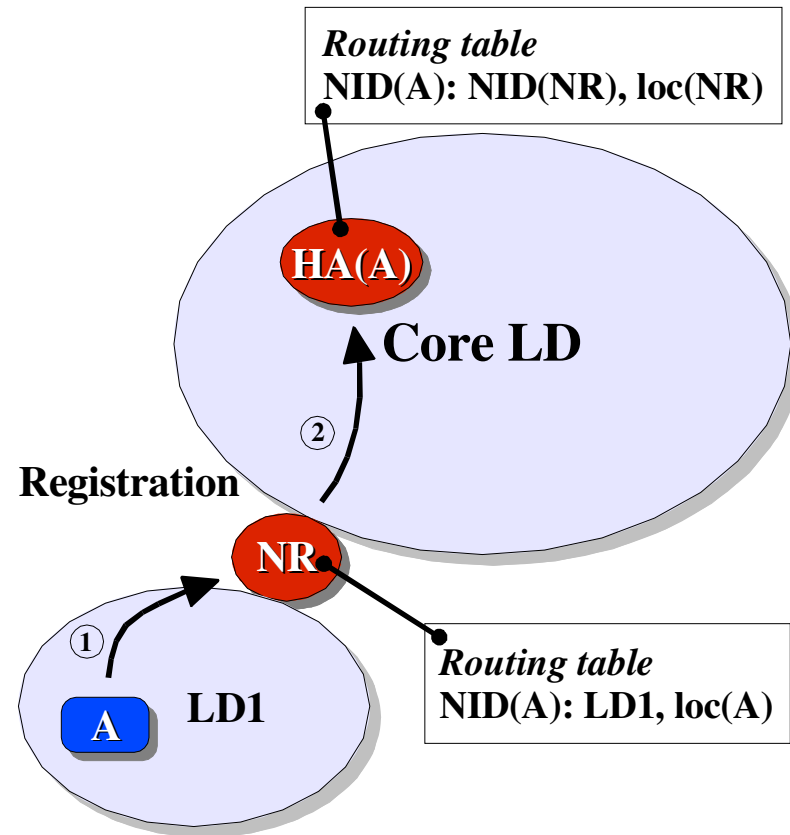
NID routers can be home agents

- ***There is no separate concept of rendezvous server or home agent***

- ▶ may however need some additional functionality
- ▶ for example: policy decision on whether to reveal location or not

- **May want explicit HA**

- ▶ registration terminates at HA
- ▶ removes need to change routing hint when node moves

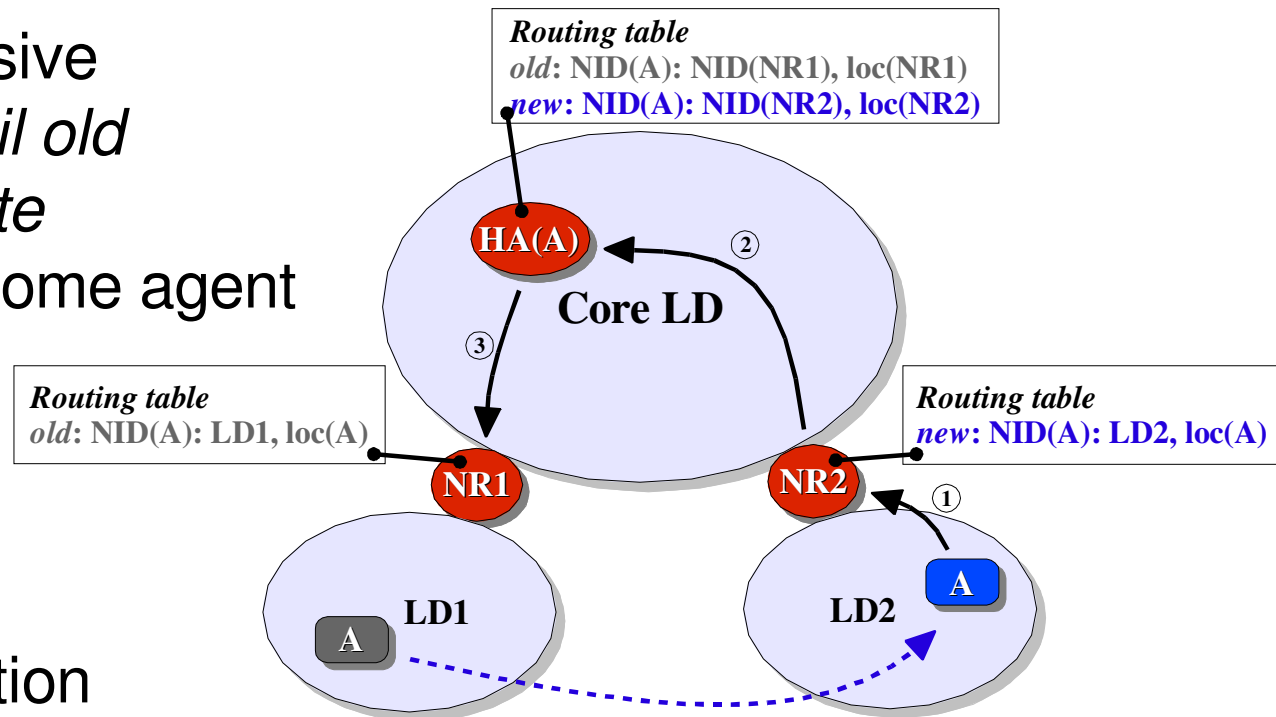


Node ID and DNS

- DNS can provide mapping from FQDN to NID and routing hint
- Assumption that this information does not change very often
- Open for other name resolution systems

Node mobility example

- A moves to another location
- (1) & (2): recursive registration *until old registration state encountered* (home agent in this case)
 - ▶ localises mobility signalling!
- (3): de-registration down old registration path



Network mobility example

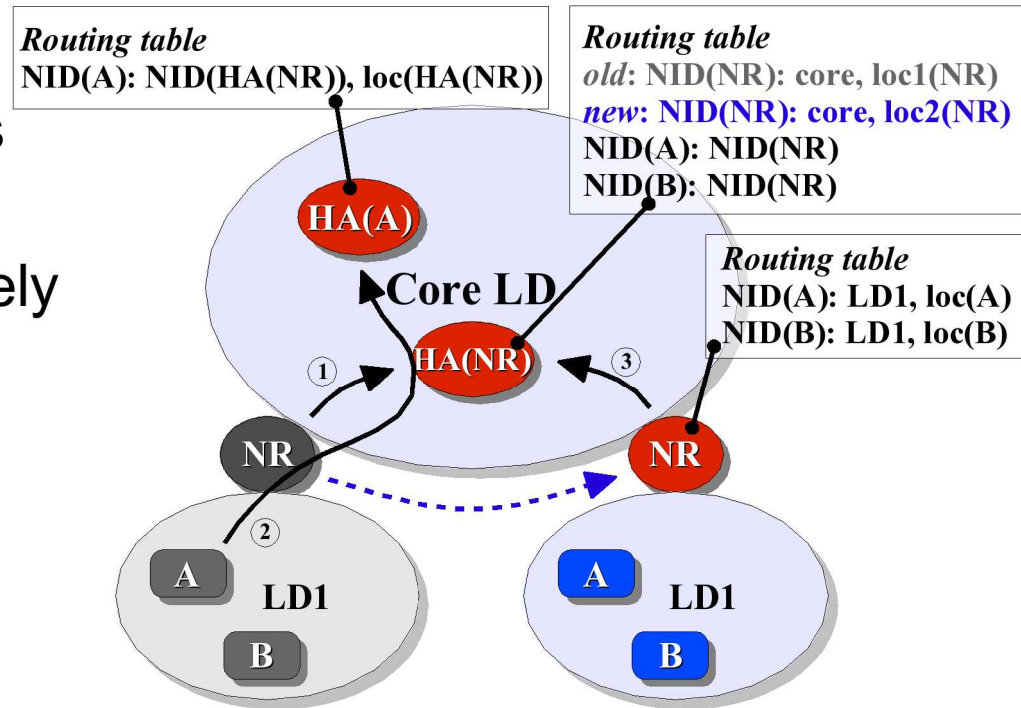
Registration:

- ▶ (1) NR registers with its home agent
- ▶ (2) A registers recursively to its home agent

Net LD1 moves to another location

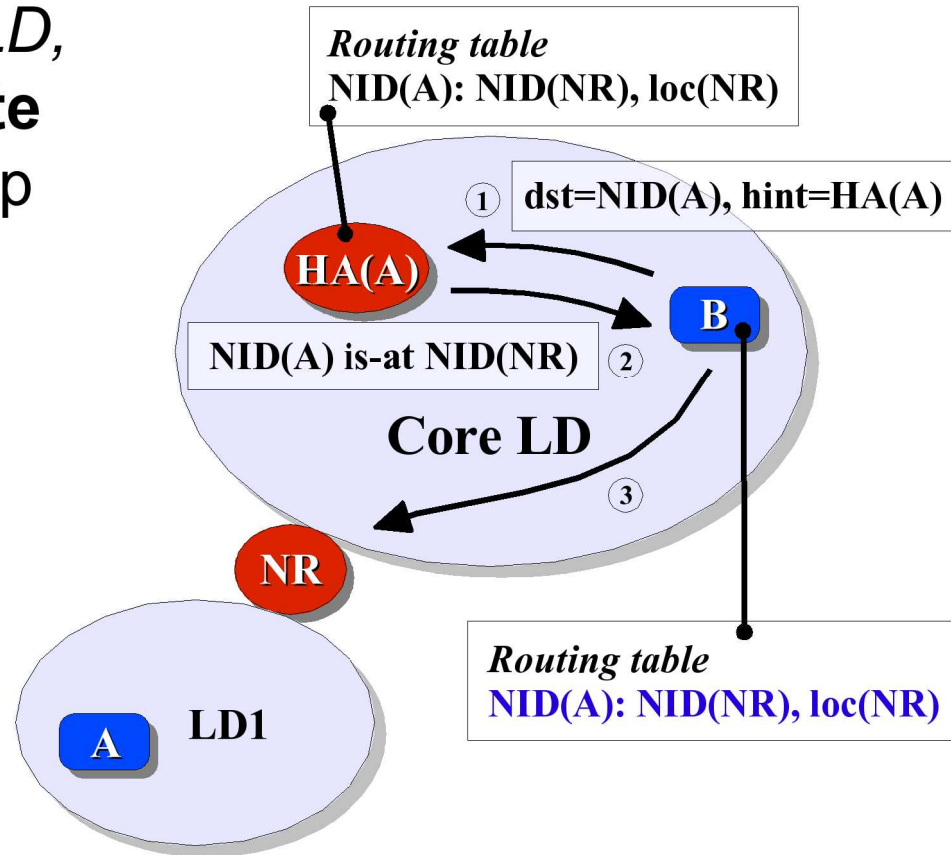
Re-registration:

- ▶ (3) Only NR needs to re-register



Route optimisation: route redirect

- If next-hop is in the same LD, a NID router can send **route redirect** to the previous hop
 - ▶ soft-state
 - ▶ same principle as ICMP redirect
- Mobility requires that NR sending redirect:
 - ▶ keeps info of redirects sent
 - ▶ notifies those when routing state changes



Multihoming

- Not fully worked out yet...
- Idea is to do multiple registrations
 - ▶ need mechanism to distinguish a new registration, replacing the old, with a multihoming registration
 - ▶ use generation number and/or timestamp

Multiple technologies

■ **Motivation**

- ▶ To completely remove the problem of migration to IPv6, the Node ID architecture needs to have a mechanism handling multiple networks of different technologies
- ▶ That would enable coexistence of IPv4 and IPv6

■ **Main idea**

- ▶ use anycast addresses on the NID routers connecting the IPv4 and IPv6 Internets

Multiple technologies – stationary nodes

■ DNS:

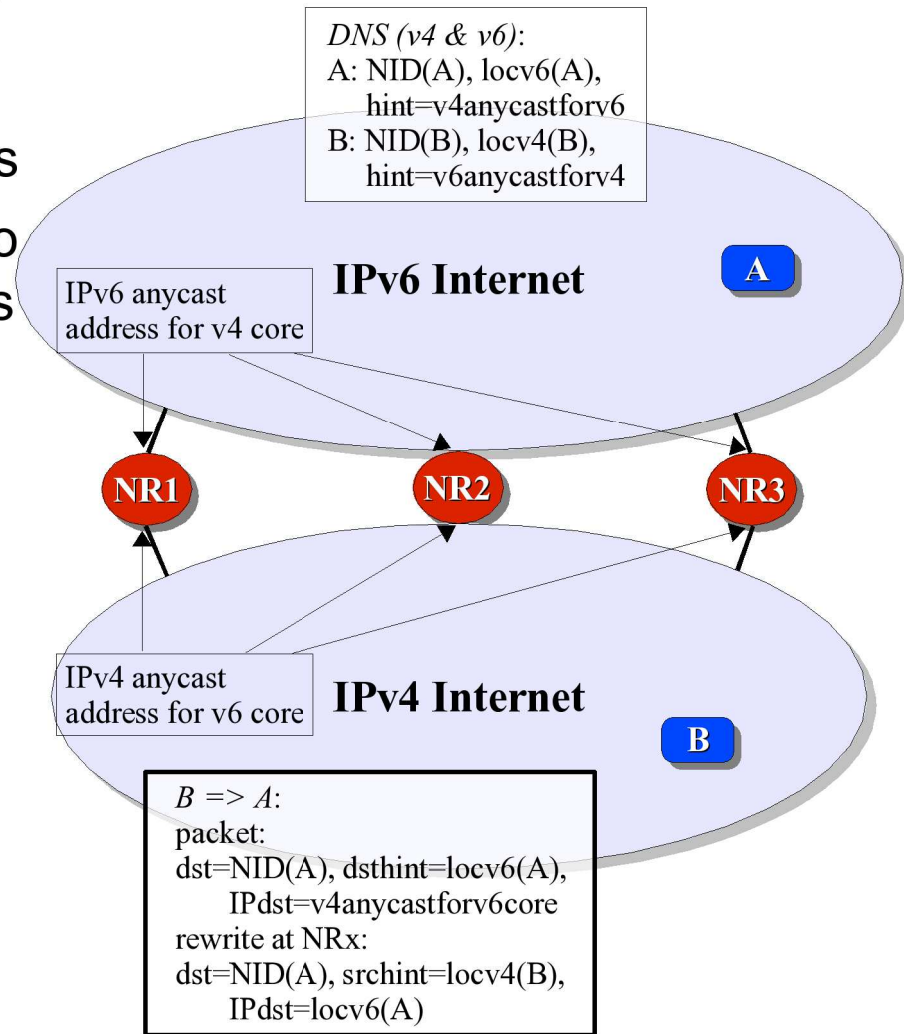
- ▶ same content in v6 & v4 worlds
- ▶ add anycast address leading to the “other side” as routing hints

■ NRx:

- ▶ gateways between v4&v6
- ▶ no routing state here!
- ▶ need session state however

■ Packet:

- ▶ put real dst locator as hint
- ▶ need srchint to find way back



State-less vs state-ful

- **Architecture described as state-less**

- ▶ that is, no session or connection state
- ▶ aka connection-less
- ▶ however requires large headers

- **Can be implemented with session setup and session state**

- ▶ different (better) security properties
- ▶ much smaller headers possible
- ▶ becomes very similar to HIP
- ▶ current prototyping done using HIP
- ▶ additional mechanism needed to update session state when NID routing state changes

Scalability issues

■ Registration state:

- ▶ NID router attaching edge network to the core has registration state for all nodes below
- ▶ limits the size of edge networks
- ▶ up to a max of perhaps a million

■ “Mobility” signalling:

- ▶ needs to be looked into further
- ▶ handwaving: *should not be worse than MIP & NEMO...*

■ Session state (state-ful case):

- ▶ session state size at NID router attaching to the core
- ▶ signalling needed to maintain state when mobile

■ *(What is missing on this slide?)*

Security issues

■ **Registration:**

- ▶ need chain of delegation certificates for the path from the node to its home agent to prevent DoS

■ **De-registration:**

- ▶ sufficient with a deregistration message signed by the node, perhaps with some generation number or timestamp?

■ **Route redirect:**

- ▶ signature by the sender of the redirect should be sufficient
- ▶ return routability check

■ *(What is missing on this slide?)*

Conclusions

- **Node ID architecture provides:**
 - ▶ bridging over heterogeneous domains (IPv4, v6, etc)
 - ▶ node and network mobility (& multihoming?)
 - ▶ NID router replacing NAT devices
 - ▶ NID router home agents can fend off unwanted traffic (DoS protection)
 - ▶ single nodes and networks can start using it
- **using *one* basic mechanism!**

Future work and more info

■ **Future work:**

- ▶ Multihoming details
- ▶ Redundant home agents
- ▶ Finish mobility mechanism in prototype

■ **More info:**

- ▶ S. Schuetz, et al., Node Identity Internetworking Architecture, draft-schuetz-nid-arch-00.txt, 2007-09-18
- ▶ Bengt Ahlgren, Jari Arkko, Lars Eggert, and Jarno Rajahalme. A node identity internetworking architecture. In Proceedings of the 9th IEEE Global Internet Symposium, Barcelona, Spain, April 28-29, 2006.